AMENDMENTS TO THE SPECIFICATION

In the Specification:

Please replace paragraphs [0015], [0026], [0041], [0046], and [0047] of the specification with the following replacement paragraphs:

[0015] In view of the above, the present invention includes real time security aspects relating to industrial control that includes integrity, confidentiality, and availability aspects. These aspects include real-time control of factory protocols based on integrity (*e.g.,* making sure a device or component reflects a commanded state), and availability (*e.g.,* can control system execute commands when requested). These aspects often include security areas that are different from non-control environment IT security concerns. Combining integrity and availability also provides the additional factory need for safety that is facilitated by the security components and protocols provided by the present invention. Confidentiality is another aspect that is becoming more important with regard to recipes, and specialized control programs (*e.g.,* protection of a special algorithm that ~~shouldn't~~ should not be disclosed to anyone (or subset of users) who has a programming device). Thus, the security mechanisms employed for lower factory protocol layers can also be applied at the "software component" level. Moreover, various security components and/or functionality can be deployed across devices and/or components that can also include nesting of security at the component level (*e.g.,* one or more security levels at device, one or more security levels at software interfacing to device, one or more security levels applied to device firmware and communications protocols).

[0026] The present invention relates to a system and methodology facilitating automation security in a networked-based industrial controller environment. Various components, systems and methodologies are provided to facilitate varying levels of automation security depending on considerations of system performance while promoting security in accordance with one or more security protocols. The security protocols can include protocol extensions that are adapted to factory networks. Dynamic security operations are provided that include[[s]] altering security patterns or interfaces based on such factors as performance, time, and the nature of network communications (*e.g.,* who is requesting or sending data). The security protocols can also

include integrity mechanisms, encryption mechanisms, session management protocols, intrusion detection components, and wireless considerations

[0041] Protocol or packet extensions can be provided in association with factory protocols such as extending the path information to include a *who* segment to identify a requester of the connection. This may take the form of an encrypted identification, certificate, public key and/or other process to identify the requester of the connection. Control devices can be adapted to verify the identity in the *who* segment in conjunction with centralized support. It is noted that identification typically involves several factors. In one aspect, ~~Identification~~ identification can be utilized for authentication (*e.g.,* something you are, have, and know). For factory level identification, the present invention can also provide "location-based" services and components. For example, components and protocols can be adapted for a "line of sight" approach for accessing a controller before actuating an output (*e.g.,* unless operator within line of site as sensed by a location sensor or wireless limitation, do not allow access to controller or limit what operator can affect). Other protocol extensions are also described in more detail below.

[0046] Turning to Fig. 3, an example security protocol 300 is illustrated in accordance with an aspect of the present invention. The security protocol 300 can be encoded within and/or associated with substantially any type of factory protocol 310 (*e.g.,* Control and Information Protocol (CIP) including DeviceNet and ControlNet, Ethernet, DH/DH+, Remote I/O, Fieldbus, Modbus, serial protocols, and so forth). The factory protocol 310 can be adapted with one or more time components at 314. The time components 314 can include time-stamp information to indicate when data has been generated and/or communicated to determine such aspects as how stale or fresh security data is (*e.g.,* the older the time stamp, the less ~~trust worthy~~ trustworthy the data).

[0047] These components 314 can also include time-limited data such as a clock value indicating how long a communication session or data transfer can last or has time remaining (*e.g.,* a number indicating that there [[is]] are so many seconds (or more or less) to transmit/receive data before having to renegotiate for further data transactions). At 318, one or more message-based components can be provided. Such components can include information

that alters or changes an associated message digest at a network device depending on the type, source, destination, and/or amount of expected communications or traffic over a network. The message digests can then be compared for unwanted alterations or changes from predetermined conditions.